AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph beginning on Line 20 of Page 5 of the specification with the following paragraph:

FIGURE 1 shows the operation of the present invention at the encrypting end of a communication channel. Data encryption is performed using two cryptographic algorithms, the first being a cryptographic pseudo random sequence generator $R()$ which is a sequence generating function and the second being a high-speed cipher $E()$, which may be relatively weak in security when used alone. The pseudo random sequence generator accepts two inputs k and v and outputs a pseudo random sequence $s = R(k, v)$. The high-speed cipher accepts a secret key s and a data segment d and produces the ciphertext $c = E(s, d)$. In addition, the illustrative embodiment uses a pre-determined function $F()$ to update an initial value, i. e., $v_i = F(V_{i-1})$. It is assumed that the encrypting end and decrypting ends share a secret key k, an initial value v_0, and the functions $F()$ and $R()$. Moreover, it is assumed that the decrypting end knows the decrypting algorithm $D()$ corresponding to the encrypting algorithm $E()$.

Please replace the paragraph beginning on Line 7 of Page 6 of the specification with the following paragraph:

At 110, the program inspects if there is any data segment available for encryption, and if not, the program terminates. Assuming that there is a data segment available, the program, at 120, increments the index i by 1, gets an updated initial value v_i using a hash function $F()$ where $v_i = F(v_{i-1})$, generates a segment key $s_i = R(k, v_i)$, and uses the segment key to encrypt the data segment to get the ciphertext segment $c_i = E(s_i, d_i)$ in a manner that is well known to those skilled in the art.